UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,918	06/29/2001	Brian Jacoby	06975-203001/Security 14	5947

26171 7590 06/15/2005

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
FLYNN, KIMBERLY D

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/894,918	**Applicant(s)** JACOBY ET AL.	
	Examiner Kimberly D. Flynn	**Art Unit** 2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-14,16,17,19,20,22,23,35,36,38,39,41-52,54,55 and 57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-14,16,17,19,20,22,23,35,36,38,39,41-52,54,55 and 57* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3/11/05; 3/7/05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to an Amendment and Reply filed March 07, 2005. Claims 1, 3-14, 16-17, 19-20, 22-23, 35-36, 38-39, 41-52, 54-55, and 57 are presented for further consideration.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on March 11, 2005 and March 11, 2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have being considered by the examiner.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox (U.S. Patent No. 6,738,814; hereinafter Cox) in view of Eichstaedt et al. (U.S. Patent No. 6,62,230; hereinafter Eichstaedt) in further view of Maher, III et al. (U.S. Patent No. 6,654,373; hereinafter Maher).

In considering claims 1-2, 4-5, 19-20, 22-23, 38-39 and 41-42, the combined system of Cox, Eichstaedt, and Maher discloses a method for securing an accessible computer system, the method comprising:

receiving more than one data packet (col. 3, lines 26-29) each includes a payload portion and an attribute portion (fig, 2 step 20 and col. 3, lines 30-33, received packets are analyzed; packets include a payload portion and an attribute portion) and are communicated between at least one access requestor (fig. 1, means 16, access requestor or attacker) and at least one access provider (fig. 1 means 12, access provider);

monitoring at least the payload portion of the data packet received by scanning the payload portion for at least one predetermined pattern (col. 3, lines 41-45);

While Cox discloses analyzing incoming packets against known patterns and denying access to the access provider by the access requestor when there is a match of the known patter, Cox does not disclose the step of counting the number of data packets that include the predetermined pattern and denying access when that number exceeds a configurable threshold. Nonetheless, denying access to client computers of data object access through a server computer when a predefined maximum value is exceeded is well known as evidenced by Eichstaedt.

In similar art Eichstaedt discloses a method for automatically limiting access of a client computer to data objects accessed through a server computer wherein when a server receives a data request (packet) from a client machine over the network, the request values of the received request having a client identifier (pattern) matching a logged entry are calculated and compared to a predefined maximum request values. If the request values exceed a corresponding predefined maximum request value, the request is refused or denied (see Eichstaedt col. 6, lines 46-61). It would have been obvious to a person having ordinary skill in the art to modify the system for blocking denial of service attacks to include the step of counting a number of data packets including a predetermined pattern in addition to matching the predetermined pattern and denying access when that number exceeds a configurable threshold in order to decrease or deny abusive traffic (i.e. denial of service attacks) thereby preventing server or website shut downs, flooding, and overloading. Attacks can cause websites to temporarily cease operation and interrupt access by legitimate consumers, it would thus be advantageous to incorporate such a system to avoid such a costly, in both time and money; non-operation period. Therefore the claimed limitations would have been obvious modifications.

Cox further discloses denying access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed the threshold number (see Cox col. 3, lines 41-54).

While Cox discloses analyzing the incoming packet against known patterns, Cox does not Explicitly disclose that the monitoring includes scanning at least the payload portion of the data packet for at least one predetermined pattern. Nonetheless, scanning the packet's payload and matching it against known patterns or strings is well known as evidenced by Maher. In similar art, Maher discloses a payload analyzer that scans the contents of data packet's payload and attempts to match the payload contents against a database of known strings (col. 2, lines 64-66).

According to Maher, the ability to look beyond the header information, while still in the fast-path and into the packet contents; would allow a network device to identify the nature of the information carried in the packet, thereby allowing much more detailed packet classification. The knowledge of the content would also allow specific contents to be identified and scanned to provide security such as virus detection, denial of service prevention, etc. It would have been obvious for a person having ordinary skill in the art, to modify the system as taught by Cox to include the step of scanning the entire packet including the payload in order to maintain an awareness of content over an entire traffic flow, and identify and filter out security problems such as email worms, viruses, denial of service attacks, and illegal hacking.

In considering claims 3, 22, and 41, the combined system of Cox, Eichstaedt, and Maher discloses that:

monitoring the data packets includes scanning the payload portion while handling the data packets with a switch (See Maher, col. 11, lines 3-17).

In considering claims 6, 25, and 44, the combined system of Cox, Eichstaedt, and Maher discloses that at least one data packet is distinguished based on an Internet address associated with the packet (See Eichstaedt col. 6, lines 46-49).

In considering claims 7, 26, and 45, the combined system of Cox, Eichstaedt, and Maher discloses that receiving the data packet includes receiving more than one data packet; and monitoring the data packet includes monitoring all of the data packets received (See Maher col. 7, lines 10-19).

In considering claims 8, 27, and 46, the combined system of Cox, Eichstaedt, and Maher discloses that the access requestor is a client (Fig. 1 (16, attacker), and the access provider is a host (Fig. 1 (12, corporate private network).

In considering claims 9-10, 28-29, and 47-48, the combined system of Cox, Eichstaedt, and Maher discloses that the data packets are monitored when communicated from the client to the host or from host to the client (See Maher col. 3, lines 39-45).

In considering claims 11, 30, and 49, the combined system of Cox, Eichstaedt, and Maher discloses that the predetermined pattern includes a login failure message communicated from the host to the client (See Maher col. 7, lines 15-17).

In considering claims 12-14, 31-33, and 50-53, although the combined system of Cox, Eichstaedt, and Maher discloses the system substantially as claimed, it does not specifically disclose that the data packets include a token-based protocol packet, a TCP packet or a PPP packet. Examiner takes official notice that the aforementioned packets are well known packets of well-known Internet protocols such as TCP and PPP. A person having ordinary skill in the art would have readily recognized the uses and advantages of including different types of protocols and their respective packets in order to comply with multiple standards thus making the system more extensible. Therefore the claimed limitation would have been an obvious modification.

In considering claims 15, 34, and 53, the combined system of Cox, Eichstaedt, and Maher discloses that controlling access includes denying access by the access requestor to the access provider (See Cox, col. 4, lines 30-33).

In considering claims 16, 35, and 54, the combined system of Cox, Eichstaedt, and Maher discloses that denying access includes affecting bandwidth for communications between the access requestor and the access provider (See Maher col. 7, lines 56-67 through col. 8, lines 1-6).

In considering claims 17, 36, and 55, the combined system of Cox, Eichstaedt, and Maher discloses that denying access includes rerouting the access requestor (See Maher col. 3, lines 25-38).

In considering claims 18-19, 37-38, 56-57, the combined system of Cox, Eichstaedt, and Maher discloses that receiving the data packet includes receiving more than one data packet; and denying access by an access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time (See Cox. col. 3, lines 11-29 and col. 4, lines 16-40).

Response to Arguments

5. Applicant's arguments with respect to claims 1, 3-14, 16-17, 19-20, 22-23, 35-36, 38-39, 41-52, 54-55, and 57 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kimberly D. Flynn whose telephone number is 571-272-3954. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on 703-305-4792. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kimberly D Flynn
Examiner
Art Unit 2153

KDF

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100